

(51) Int.Cl.⁶

識別記号

F I

H 0 4 L 9/32

G 0 6 F 13/00

H 0 4 L 9/08

3 5 1

H 0 4 L 9/00

G 0 6 F 13/00

H 0 4 L 9/00

6 7 5 B

3 5 1 Z

6 0 1 C

審査請求 未請求 請求項の数11 O L (全 13 頁)

(21) 出願番号

特願平10-89097

(22) 出願日

平成10年(1998)4月1日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 西村 拓也

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 飯塚 裕之

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 山田 正純

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 弁理士 松田 正道

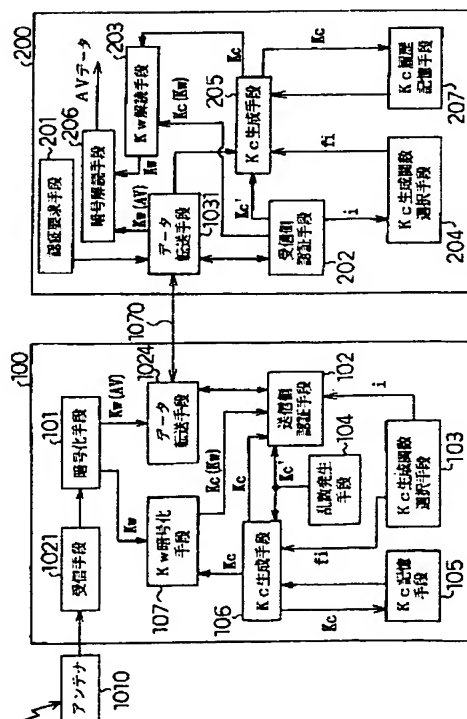
最終頁に続く

(54) 【発明の名称】 データ送信装置、データ受信装置、及び媒体

(57) 【要約】

【課題】 コントロールキー K_c が不正に解読されると、それで暗号化されているワークキー K_w も解読されるため、AVデータが不正に解読されるという課題。

【解決手段】 STB100は、受信手段1021からのAVデータをワークキー K_w により暗号化する暗号化手段101と、VTR装置200と認証動作を行い、 K_c の暗号化を行う送信側認証手段102と、 K_c を生成するために、複数の関数とその関数識別子を予め内蔵し、何れかの関数を選択する K_c 生成関数選択手段103と、 K_c を生成する際に利用する乱数 K_c' を発生させる乱数発生手段104と、既に生成された K_c を記憶する K_c 記憶手段105と、過去に生成された K_c の一部と、上記出力された乱数 K_c' と、それらを変数とする上記選択された関数 f_i とを利用して、新たな K_c を生成する K_c 生成手段106と、生成された K_c を用いて K_w を暗号化する K_w 暗号化手段107手段等を備える。



【特許請求の範囲】

【請求項1】 データ受信装置からのデータ転送要求を受け付ける転送要求受付手段と、
前記転送要求に基づいて、前記データ受信装置にデータの転送を行うデータ転送手段と、
前記転送されるデータを所定のワークキーKwに基づいて暗号化する第1暗号化手段と、
そのワークキーKwをコントロールキーKcに基づいて暗号化し、前記データ受信装置へ送る第2暗号化手段と、
前記コントロールキーKcの生成に利用する秘密要素を発生させる秘密要素発生手段と、
過去に生成されたコントロールキーKcの全部又は一部と前記発生された秘密要素と、それらを変数とする第1の関数とを利用して、新たなコントロールキーKcを生成するコントロールキー生成手段とを備え、
前記コントロールキーKcが新たに更新される場合、前記秘密要素を、前記第1の関数を有する前記データ受信装置に転送するものであることを特徴とするデータ送信装置。

【請求項2】 データ受信装置からのデータ転送要求を受け付ける転送要求受付手段と、
前記転送要求に基づいて、前記データ受信装置にデータの転送を行うデータ転送手段と、
前記転送されるデータを所定のワークキーKwに基づいて暗号化する第1暗号化手段と、
そのワークキーKwをコントロールキーKcに基づいて暗号化し、前記データ受信装置へ送る第2暗号化手段と、
新たなコントロールキーKcを生成するコントロールキー生成手段と、
過去に生成されたコントロールキーKcの全部又は一部と前記新たに生成されたコントロールキーKcと、それらを変数とする第2の関数とを利用して、秘密要素を生成する秘密要素生成手段とを備え、
前記コントロールキーKcが新たに更新される場合、前記秘密要素を、前記第2の関数の逆関数を有する前記データ受信装置に転送するものであることを特徴とするデータ送信装置。

【請求項3】 請求項1又は2記載のデータ送信装置にデータ転送要求を行う転送要求手段と、
前記転送要求に基づいて前記データ送信装置から転送されてくる暗号化されたワークキーKwを、コントロールキーKcで解読するとともに、暗号化されたデータを、そのワークキーKwに基づいて解読する暗号解読手段と、
前記ワークキーKwの解読に既に利用された前記コントロールキーKcを履歴情報として記憶する履歴情報記憶手段と、
前記第1の関数又は前記逆関数を格納する関数格納手段

と、
前記格納されている第1の関数又は逆関数と、前記履歴情報記憶手段に記憶されている過去のコントロールキーKcの全部又は一部と、請求項1又は2記載の前記データ送信装置から転送されてくる前記秘密要素とに基づいて、新たなコントロールキーKcを生成するコントロールキー生成手段と、を備えたことを特徴とするデータ受信装置。

【請求項4】 前記データ送信装置が別のデータ受信装置と既に前記データの転送を行っている途中から、データの転送を要求する場合、
前記コントロールキー生成手段により初期段階で利用される前記過去のコントロールキーKcは、前記履歴情報記憶手段に記憶されている前記コントロールキーKcではなく、前記データ送信装置から転送されてくるコントロールキーKcであることを特徴とする請求項3記載のデータ受信装置。

【請求項5】 前記転送を行う旨が決定された場合、前記データ受信装置が有する前記第1の関数又は前記逆関数の変数が、コントロールキーKcを生成するのに不足している時期においては、前記コントロールキーKcを含む暗号情報を初期情報として、前記データ受信装置に転送することを特徴とする請求項1又は2記載のデータ送信装置。

【請求項6】 前記転送を行う旨が決定された場合、前記データ受信装置が有する前記第1の関数又は前記逆関数の変数が、コントロールキーKcを生成するのに不足している時期においては、前記秘密要素を含む前記不足している変数を初期情報として前記データ受信装置に転送することを特徴とする請求項1又は2記載のデータ送信装置。

【請求項7】 前記転送を行う旨が決定された場合、前記データ受信装置が有する前記第1の関数又は前記逆関数の変数が、コントロールキーKcを生成するのに不足している時期の内、(1)前半においては、前記コントロールキーKcを含む暗号情報を初期前半情報として、又、(2)後半においては、前記秘密要素を含む前記不足している変数を初期後半情報として前記データ受信装置に転送することを特徴とする請求項1又は2記載のデータ送信装置。

【請求項8】 前記第1の関数又は前記逆関数の変数が、コントロールキーKcを生成するのに不足している時期においては、請求項5記載のデータ送信装置から転送されてくる前記初期情報を解読し、前記コントロールキーKcを抽出する抽出手段を備え、
前記暗号解読手段が、前記抽出されたコントロールキーKcを前記解読に利用することを特徴とする請求項3記載のデータ受信装置。

【請求項9】 前記第1の関数又は前記逆関数の変数が、コントロールキーKcを生成するのに不足している

1は、データ転送手段1024と同様の手段であり、暗号化されたワークキー及び暗号化されたAVデータを受け取る手段である。認証手段1032は、固有の秘密関数Saを予め有しており、認証作業の結果として、サブキーKsaを生成して、復号化手段1033へ出力する手段である。復号化手段1033は、データ転送手段1031から得た暗号化されたコントロールキーKsa

(Kc)をサブキーKsaにより復号し、この復号化されたコントロールキーKcにより、暗号化されたワークキーKc(Kw)を復号し、その復号化されたワークキーKwにより、暗号化されたAVデータKw(AV)を復号する手段である。記録・再生手段1034は、復号化されたAVデータを記録し、又、その記録データを再生する手段である。

【0015】尚、その他の端末装置である、VTR装置(B)1040、記録装置(D)1050、TV装置(D)1060も、記録・再生手段を除き、上記VTR装置(A)1030の構成と基本的に同じである。但し、各認証手段が予め有する秘密関数は、上記各装置の順番でいえば、Sb、Sc、Sdである。従って、各装置と、STB1020との認証作業により生成されるサブキーは、上記の順番でいえば、Ksb、Ksc、Ksdである。

【0016】以上の構成において、次に、認証・鍵交換の内容を簡単に述べる。尚、本明細書では、認証の成立の結果としてサブキーKsxを生成するまでの作業、及びその後に行うコントロールキーKcの転送・受理の作業を含む一連の作業をまとめて、認証・鍵交換というものとする。

【0017】例えば、VTR装置(A)1030からSTB1020に対して、AVデータの転送要求を行う場合、その実行に先立ち次のような複雑な認証作業が必要となる。

【0018】ステップ1001：即ち、先ず、VTR装置(A)1030の認証手段1032が、乱数A1、A2を発生させ、これを秘密関数Saにより暗号化する。ここで、暗号化された乱数をSa(A1、A2)と記載する。認証手段1032は、Sa(A1、A2)と自己の識別番号Idaとをデータ転送手段1031を介して、STB1020へ転送する。ここで、識別番号は、各端末装置固有の番号で予め与えられている。

【0019】ステップ1002：STB1020では、認証手段1023がデータ転送手段1024を介して、Sa(A1、A2)と識別番号Idaとを得て、その識別番号を認識して、それに対応する秘密関数Saを、保有している複数の秘密関数の中から選択する。これにより、STB1020が、VTR装置(A)1030との間で認証に使用すべき秘密関数が特定される。

【0020】ステップ1003：次に、STB1020の認証手段1023が、秘密関数Saを用いて、上記受

信したSa(A1、A2)を解読し、A1、A2を復元して、後者の乱数A2のみを、暗号化せずにVTR装置(A)1030へ送り返す。

ステップ1004：次に、VTR装置(A)1030の認証手段1032が、STB1020から送り返されてきた乱数A2と、自らが、上記ステップ1001で発生させた乱数A2とを比較する。双方の乱数が一致すれば、STB1020が正規の装置であると判断出来る。

【0021】ステップ1005：次に、STB1020側の認証手段1023が、乱数B1、B2を発生させ、これを秘密関数Saにより暗号化する。そして、Sa(B1、B2)をVTR装置(A)1030へ転送する。

【0022】ステップ1006：VTR装置(A)1030では、認証手段1032が秘密関数Saを用いて、上記受信したSa(B1、B2)を解読し、B1、B2を復元して、後者の乱数B2のみを、暗号化せずにSTB1020へ送り返す。

【0023】ステップ1007：次に、認証手段1023が、VTR装置(A)1030から送り返されてきた乱数B2と、自らが、上記ステップ1005で発生させた乱数B2とを比較する。双方の乱数が一致すれば、VTR装置(A)1030が正規装置であると判断出来る。

【0024】以上により、認証が成立したことになる、双方が互いに相手装置が正規の装置であることを確認出来る。その結果、VTR装置(A)1030へのAVデータの転送が許可される。

【0025】この認証作業の結果、4つの乱数A1、A2とB1、B2が、双方の装置の認証手段1023、1032に発生している。

【0026】そこで、次に、双方の認証手段1023、1032がそれぞれ、乱数A1、B1を用いて上記サブキーKsaを生成する。尚、サブキーKsaの生成に際し、乱数A2、B2を使用しないのは、これらは、暗号化せずに転送されたという経緯があるため、その様な経緯の無い乱数A1、B1を使用する方が、キーの安全性から見て、より優れているからである。

【0027】暗号化手段1022では、この様にして生成されたサブキーKsaを用いて、コントロールキーKcが暗号化され、又、コントロールキーKcを用いてワークキーKwが暗号化される。これらは、認証手段1023へ送られる。又、AVデータはワークキーKwで暗号化されて、データ転送手段1024へ送られる。

【0028】そして、上記暗号化されたコントロールキーKsa(Kc)と、暗号化されたワークキーKc(Kw)が、認証手段1023からデータ転送手段1024を介してVTR装置(A)1030へ転送される。その後、暗号化されたAVデータKw(AV)がデータ転送手段1024から、VTR装置(A)1030へ転送さ

れる。

【0029】一方、VTR装置(A)1030では、復号化手段1033が、先ず、認証手段1032から得たサブキーKsaを用いて、暗号化されたコントロールキーKsa(Kc)の復号を行う。次に、復号されたコントロールキーKcを用いて暗号化されたワークキーKc(Kw)の復号を行う。更に、この様にして復号されたワークキーKwを用いて、暗号化されたAVデータKw(AV)を復号するものである。

【0030】尚、STB1020が、使用するワークキーKwは、転送データの安全性を確保するために、データ転送中において定期的に変更される。

【0031】従って、ワークキーKwが変更される度に、暗号化された新たなワークキーKwが、STB1020からデータ転送中の端末装置へ送られる。

【0032】

【発明が解決しようとする課題】しかしながら、このような従来のデータ転送のやり方では、仮に、コントロールキーKcが不正者によって解読されたとすると、コントロールキーKcで暗号化されているワークキーKwも解読されてしまうため、結果的に、暗号化されたAVデータが、不正者によって解読されることになるという課題を有していた。

【0033】この場合、コントロールキーKcを更新することが考えられるが、上述したとおり、従来は、認証・鍵交換の一環として、コントロールキーKcを転送するものであるから、ただ単にコントロールキーKcを更新するとなると、認証・鍵交換の動作を更新の度に行う必要がある。

【0034】しかし、認証・鍵交換の動作をKcの更新の度に再度行うとなると、新たなサブキーを生成するまでの上記一連の処理等が、双方の装置にとって大きな負担となる。そこで、本願発明者は、認証・鍵交換の動作による負担を従来に比べて実質上増やすことなく、コントロールキーKcを更新することにより、コントロールキーKcのセキュリティを向上することを考えたものである。

【0035】本発明は、上述した課題を考慮して、従来に比べて実施上の負担を増やすことなくコントロールキーKcの秘密保持についての信頼性を従来に比べてより一層向上させることが出来るデータ送信装置、データ受信装置、及び媒体を提供することを目的とする。

【0036】

【課題を解決するための手段】請求項1記載の本発明は、データ受信装置からのデータ転送要求を受け付ける転送要求受付手段と、前記転送要求に基づいて、前記データ受信装置にデータの転送を行うデータ転送手段と、前記転送されるデータを所定のワークキーKwに基づいて暗号化する第1暗号化手段と、そのワークキーKwをコントロールキーKcに基づいて暗号化し、前記データ

受信装置へ送る第2暗号化手段と、前記コントロールキーKcの生成に利用する秘密要素を発生させる秘密要素発生手段と、過去に生成されたコントロールキーKcの全部又は一部と前記発生された秘密要素と、それらを変数とする第1の関数とを利用して、新たなコントロールキーKcを生成するコントロールキー生成手段とを備え、前記コントロールキーKcが新たに更新される場合、前記秘密要素を、前記第1の関数を有する前記データ受信装置に転送するものであるデータ送信装置である。

【0037】請求項2記載の本発明は、データ受信装置からのデータ転送要求を受け付ける転送要求受付手段と、前記転送要求に基づいて、前記データ受信装置にデータの転送を行うデータ転送手段と、前記転送されるデータを所定のワークキーKwに基づいて暗号化する第1暗号化手段と、そのワークキーKwをコントロールキーKcに基づいて暗号化し、前記データ受信装置へ送る第2暗号化手段と、新たなコントロールキーKcを生成するコントロールキー生成手段と、過去に生成されたコントロールキーKcの全部又は一部と前記新たに生成されたコントロールキーKcと、それらを変数とする第2の関数とを利用して、秘密要素を生成する秘密要素生成手段とを備え、前記コントロールキーKcが新たに更新される場合、前記秘密要素を、前記第2の関数の逆関数を有する前記データ受信装置に転送するものであるデータ送信装置である。

【0038】請求項3記載の本発明は、請求項1又は2記載のデータ送信装置にデータ転送要求を行う転送要求手段と、前記転送要求に基づいて前記データ送信装置から転送されてくる暗号化されたワークキーKwを、コントロールキーKcで解読するとともに、暗号化されたデータを、そのワークキーKwに基づいて解読する暗号解読手段と、前記ワークキーKwの解読に既に利用された前記コントロールキーKcを履歴情報として記憶する履歴情報記憶手段と、前記第1の関数又は前記逆関数を格納する関数格納手段と、前記格納されている第1の関数又は逆関数と、前記履歴情報記憶手段に記憶されている過去のコントロールキーKcの全部又は一部と、請求項1又は2記載の前記データ送信装置から転送されてくる前記秘密要素とに基づいて、新たなコントロールキーKcを生成するコントロールキー生成手段とを備えたデータ受信装置である。

【0039】請求項11記載の本発明は、上記の何れか一つに記載の各手段の全部又は一部の手段をコンピュータに実行させるためのプログラムを記録した媒体である。

【0040】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【0041】(第1の実施の形態)図1は、本発明の一

実施の形態におけるデータ送信装置及びデータ受信装置の構成を示す構成図であり、以下に、同図を参照しながら、本実施の形態の構成について述べる。尚、本実施の形態では、図6で説明したものと、基本的に同じ構成のものには、同じ符号を付し、その詳細な説明は省略した。

【0042】図1に示すSTB100には、既に述べた図6と同様に、データ受信端末装置としてVTR装置

(a) 200、VTR装置 (b) 300、記録装置 (c) 400及びTV装置 (d) 500が接続されている構成である。尚、図1では、説明の都合上、端末装置としてVTR装置 (a) 200のみを記載し、他の端末装置の記載を省略した。これら記載を省略した端末装置300～500は、以下に述べるVTR装置 (a) 200の構成と基本的に同様の構成を備えている。

【0043】同図において、先ず、STB100の構成を述べる。

【0044】即ち、暗号化手段101は、受信手段1021からのAVデータをワークキーKwにより暗号化する手段である。送信側認証手段102は、端末装置との間で認証・鍵交換を行う手段である。又、送信側認証手段102は、認証動作においてサブキーを生成し、初回のみ、その生成したサブキーを用いて複数個のコントロールキーKcを暗号化する手段である。Kc生成関数選択手段103は、コントロールキーKcを生成するために、 $f_1 \sim f_m$ のm個の関数と、それに対応する関数識別子1～mを予め内蔵しており、何れか一つの関数 f_i を選択する手段である。又、Kc生成関数選択手段103は、Kc生成手段106に対しては、選択した関数 f_i を出力し、送信側認証手段102に対しては、対応する関数識別子iを出力する手段である。乱数発生手段104は、コントロールキーKcの生成に利用される乱数Kc'を発生し、出力する手段である。Kc記憶手段105は、既に生成されたコントロールキーKcを記憶する手段である。Kc生成手段106は、Kc記憶手段106から送られてくる、過去に生成された幾つかのコントロールキーKcの一部と、上記出力された乱数Kc'と、それらを変数とする上記出力された関数 f_i とを利用して、新たなコントロールキーKcを生成する手段である。ここで、関数 f_i の変数となるコントロールキーKcの一部とは、本実施の形態では、1つ前と、2つ前に生成したキーである。尚、この関数については、更に後述する。Kw暗号化手段107は、生成されたコントロールキーKcを用いてワークキーKwを暗号化する手段である。

【0045】本実施の形態では、コントロールキーKcが、次々と更新されるので、データ転送の開始に際し、最初に使用されるコントロールキーをKc[1]と表し、更新の結果、n番目に使用されるコントロールキーをKc[n]と表すものとする。又、同様にして、Kc[n+1]を生成するために利用された乱数をKc'[n]と表すものとする。但し、nは、自然数とする。

【0046】従って、本実施の形態では、上記関数 f_i は、次のような式(数1)で表せる。

【0047】

【数1】 $f_i(Kc'[n], Kc[n-1], Kc[n])$

ここで、nは、自然数とする。

【0048】よって、n+1番目に生成されるコントロールキーKc[n+1]は、次の式(数2)で表せる。

【0049】

【数2】 $Kc[n+1] = f_i(Kc'[n], Kc[n-1], Kc[n])$

ここで、nは、自然数とする。

【0050】尚、本発明の転送要求受付手段は、データ転送手段1024及び送信側認証手段102を含む手段である。又、本発明のデータ転送手段は、データ転送手段1024及び暗号化手段101を含む手段である。本発明の第1暗号化手段は、暗号化手段101に、又、第2暗号化手段は、Kw暗号化手段107に対応する。本発明の秘密要素発生手段は、乱数発生手段104に対応し、本発明の第1関数は、関数 f_i に対応する。また、送信側認証手段102は、図6で述べた認証手段1023と同様に、秘密関数(Sa、Sb、Sc、Sd、・・・、Sx)を有している。

【0051】次に、VTR装置200の構成について述べる。

【0052】即ち、同図において、認証要求手段201は、STB100に対して、データ転送の要求をするために認証要求を行う手段である。受信側認証手段202は、STB100との間で認証・鍵交換を行う手段である。又、受信側認証手段202は、認証動作においてサブキーを生成し、認証動作の結果として送られてくる、暗号化された複数個のコントロールキーKcをそのサブキーにより解読し、その解読結果の中から、コントロールキーKc[1]を抽出し、Kw解読手段203に出力する手段である。又、受信側認証手段202は、暗号化されたワークキーKwを受理して、Kw解読手段203に送る手段である。更に又、受信側認証手段202は、STB100から送られてくる関数識別子iをKc生成関数選択手段204に、又、乱数Kc'[n]をKc生成手段205に出力する手段である。

【0053】暗号解読手段206は、STB100から転送されてきた暗号化されたAVデータをワークキーKwを用いて解読し、記録・再生手段(図示省略)1034へ出力する手段である。Kc生成関数選択手段204は、STB100が内蔵している上記複数個の関数と同じ関数を、予め内蔵しており、入力されてきた関数識別子iに対応する関数 f_i を抽出して、Kc生成手段205へ出力する手段である。この関数 f_i は、数1で表せる。Kc生成手段205は、Kc履歴記憶手段207か

ら読み出した1つ前と2つ前に使用していたコントロールキーKcと、受信側認証手段202から出力された乱数Kc'とを、関数fiの変数として利用して、新たなコントロールキーKcを生成する手段である。この新たなKcは、数2で表せる。又、Kc履歴記憶手段207は、Kc生成手段205により生成されたコントロールキーKcの履歴を記憶しておく手段である。尚、STB100と他の端末装置との間で、既にデータの転送が行われている最中に、VTR装置200が途中からデータの転送を受ける場合には、Kc履歴記憶手段207は、次のような例外的な動作を行う手段である。即ち、その場合、Kc履歴記憶手段207は、上記他の端末装置との間で現に使用しているコントロールキーと、その1つ前に使用していたコントロールキーとをSTB100から受け取り、それらを記憶する手段である。

【0054】尚、受信側認証手段202は、図6で述べた、認証手段1032と同様に、秘密関数Saを有している。

【0055】以上の構成において、次に、図1、図2を参照しながら、本実施の形態の動作を説明する。

【0056】ここでは、まず、(1) STB100が、VTR装置200のみに対してAVデータの転送を開始する場合を述べ、その後、(2) 上記(1)の動作中に、別の受信端末装置すなわち、記録装置400に対するデータ転送が開始される場合を中心に説明する。

【0057】(1) 上述した通り、ここでは、STB100からVTR装置200へのみ、AVデータを転送する場合について述べる。

【0058】VTR装置200が、所望のAVデータをSTB100から転送してもらうためには、STB100とVTR装置200との間で、図6で述べたのと同様の認証・鍵交換の動作を行った後、本実施の形態の特有の動作を行うものである。

【0059】ステップ101：即ち、ここでは、認証要求手段201により、STB100に対して認証・鍵交換の動作の開始の要求が行われる。その後の認証・鍵交換の動作の詳細は、以下の点を除き、上述したステップ1001～1007で述べたものと同様であるので、その説明は省略する。尚、この認証・鍵交換の動作においては、VTR装置200における乱数A1、A2の発生は、受信側認証手段202が行い、STB100における乱数B1、B2の発生は、乱数発生手段104が行う。又、上記ステップ1001～1007の動作において、認証が成立した場合、図6で述べた通り、双方の装置においてサブキーKsaが生成される。その後の、認証・鍵交換の動作において最初にVTR装置200へ転送されるキーは、本実施の形態では、ステップ102で述べるように2個であり、この点は従来と異なる。

【0060】ステップ102：即ち、乱数発生手段104で発生された2つの乱数をダミーキーKc[0]と、コ

ントロールキーKc[1]と定義する。このダミーキーKc[0]と、コントロールキーKc[1]は、送信側認証手段102へ送られる。又、コントロールキーKc[1]は、Kw暗号化手段107にも送られる。

【0061】即ちこの場合、Kc[0]、及びKc[1]の生成については、数2を使用せず、例外的処置として、乱数発生手段104により発生される乱数を使用するものとする。

【0062】ステップ103：さらに、これら2つのキーKc[0]及びKc[1]は、Kc記憶手段105に記憶される。又、Kc生成関数選択手段103により選択された関数fiが、Kc生成手段106に送られ、それに対応する関数識別子iが送信側認証手段102に送られる。尚、関数fiは、必要に応じて、更新しても良い。

【0063】ステップ104：送信側認証手段102では、上記のようにして送られてきたダミーキーKc[0]とコントロールキーKc[1]が、サブキーKsaにより暗号化されて、Ksa(Kc[0]、Kc[1])として、データ転送手段1024へ送られる。さらに、Ksa(Kc[0]、Kc[1])は、データ転送手段1024から、VTR装置200へ転送される。図2では、この転送に、符号601を付した。ここで、図2は、コントロールキーの更新に伴い行われる、STB100から受信端末装置200、400への転送の状況を中心に示した模式図である。同図において、縦軸は時間であり、図中の上から下へ向けて時間が経過している。

【0064】尚、この転送601の際、Kc生成関数fiに対応する関数識別子iも、VTR装置200に転送される。

【0065】ステップ105：STB100から転送されてきたKsa(Kc[0]、Kc[1])と関数識別子iは、データ転送手段1031により、受信側認証手段202へ送られる。

【0066】ステップ106：そして、受信側認証手段202は、Ksa(Kc[0]、Kc[1])を解読し、前後に配置された2つのキーの内、予め定められている通り、後ろに配置されたKc[1]を抽出し、Kw解読手段203へ送る。又、受信側認証手段202は、関数識別子iをKc生成関数選択手段204へ送る。そして、Kc生成関数選択手段204が、その識別子iに対応する関数fiを抽出して、Kc生成手段205へ送る。尚、解読されたKc[0]、Kc[1]は、共に、Kc生成手段205を介して、Kc履歴記憶手段207に送られ、記憶される。

【0067】ステップ107：一方、Kw暗号化手段107がコントロールキーKc[1]を用いて暗号化したワークキー、即ち、Kc[1](Kw)は、送信側認証手段102及びデータ転送手段1024を経て、VTR装置200に転送される。

【0068】ステップ108：VTR装置200に送ら

れてきた $Kc[1]$ (Kw) は、受信側認証手段202を経て、 Kw 解読手段203に送られる。 Kw 解読手段203は、ステップ106において送られてきたコントロールキー $Kc[1]$ を用いて、 $Kc[1]$ (Kw) を解読して、 Kw を暗号解読手段206に送る。

【0069】ステップ109：一方、STB100の暗号化手段101により暗号化されたAVデータである Kw (AV) の転送が、データ転送手段1024を介して開始される。

【0070】ステップ110： Kw (AV) は、データ転送手段1031から暗号解読手段206へ送られる。暗号解読手段206は、 Kw 解読手段203から送られてきた Kw を用いて、 Kw (AV) を解読し、記録・再生手段に出力する。

【0071】次に、ステップ110において、解読されたAVデータが記録・再生手段に出力されている途中で、コントロールキー Kc が更新される場合の動作を述べる。

【0072】ステップ201：本実施の形態では、コントロールキーを定期的に更新するものとし、乱数発生手段104が、乱数 Kc' を定期的に発生させる。即ち、1回目の更新に利用する乱数 $Kc'[1]$ が、乱数発生手段104から Kc 生成手段106と、送信側認証手段102に送られる。

【0073】ステップ202：送信側認証手段102に送られた乱数 $Kc'[1]$ は、データ転送手段1024を介して、VTR装置200へ転送される。図2では、この転送に符号602を付した。

【0074】ステップ203： Kc 生成手段106は、 Kc 記憶手段105に記憶されている $Kc[0]$ 及び $Kc[1]$ を読み出して、乱数発生手段104から送られてきた乱数 $Kc'[1]$ と共に、関数 f_i (数2参照) の変数として用いる。

【0075】この場合、生成される新たなコントロールキー $Kc[2]$ は、数2より、 $Kc[2]=f_i(Kc'[1], Kc[0], Kc[1])$ と表せる。尚、 $Kc[2]$ は、 Kc 記憶手段105に記憶される。

【0076】ステップ204：新たなコントロールキー $Kc[2]$ は、 Kw 暗号化手段107へ送られ、ワークキー Kw の暗号化に用いられる。暗号化されたワークキーである $Kc[2]$ (Kw) は、ステップ107と同様にしてVTR装置200へ転送される。

【0077】ステップ205：又、ステップ202において、VTR装置200に転送された乱数 $Kc'[1]$ は、データ転送手段1031から受信側認証手段202に送られ、さらに Kc 生成手段205に送られる。

【0078】ステップ206： Kc 生成手段205では、 Kc 履歴記憶手段207に記憶されている $Kc[0]$ 及び $Kc[1]$ を読み出して、ステップ205において送られてきた乱数 $Kc'[1]$ と共に、関数 f_i (数2参

照) の変数として用いる。この場合、生成される新たなコントロールキー $Kc[2]$ は、ステップ203で述べたものと同じであり、 $Kc[2]=f_i(Kc'[1], Kc[0], Kc[1])$ と表せる。尚、 $Kc[2]$ は、 Kc 履歴記憶手段207に記憶される。

【0079】ステップ207：新たなコントロールキー $Kc[2]$ は、 Kw 解読手段203へ送られ、 $Kc[2]$ で暗号化されたワークキー Kw の解読に用いられる。解読されたワークキー Kw は暗号化解読手段206に送られる。

【0080】ステップ208：ステップ110と同様の動作が行われる。

【0081】次に、ステップ208において、解読されたAVデータが記録・再生手段に出力されている途中で、コントロールキー $Kc[2]$ が、さらに更新される場合の動作を述べる。ここでは、すでに述べた内容と同様の点が多いので、数2に関する特徴点のみについて述べる。

【0082】即ち、ここで生成されるコントロールキー $Kc[3]$ は、数2の n に2を代入することにより次のように表せる。図2では、乱数 $Kc'[2]$ の転送に符号603を付した。

【0083】

【数3】

$Kc[3]=f_i(Kc'[2], Kc[1], Kc[2])$
上記(数3)及び(数2)から明らかなように、本実施の形態においては、2回目の更新以降に生成されるコントロールキーは、1つ前、及び2つ前に使用したコントロールキーと、乱数発生手段104により更新の度に発生される乱数 Kc' と、それらを変数とする関数 f_i とにより生成されるものである。

【0084】以上述べた様に、本実施の形態によれば、認証動作を繰り返すことなく、過去に使用したコントロールキーの履歴と乱数とを用いてコントロールキーを更新することにより、コントロールキーの信頼性をより一層向上させることが出来る。

【0085】(2) 上記(1)の動作において、コントロールキーの2回目の更新が行われた後に、記録装置400に対するデータ転送が開始される場合について、図2を参照しながら述べる。

【0086】ステップ301：STB100と、新たに転送要求を行う記録装置400との間において、ステップ101と同様の認証動作が行われる。

【0087】ステップ302：認証が成立した後、送信側認証手段102は、 Kc 記憶手段105に記録されている、現在使用中のコントロールキー $Kc[3]$ とその1つ前に使用していたコントロールキー $Kc[2]$ とを読み出して、サブキー Ksc により暗号化する。そして、この $Ksc(Kc[2], Kc[3])$ と、現在使用中の関数 f_i に対応する関数識別子 i とをデータ転送手段102

4を介して、記録装置400へ転送する(図2では、この転送に符号604を付した)。尚、サブキーKscは、上記認証動作により上記と同様の方法により生成されたものである。

【0088】ステップ303:記録装置400では、受信側認証手段202が、上記のようにして送られてきたKsc(Kc[2]、Kc[3])を、サブキーKscを用いて解読し、Kc[3]を抽出する。この解読・抽出の動作と、その後のKc生成関数選択手段204及びKc履歴記憶手段207などの動作は、ステップ106で述べた内容と同じである。

【0089】ステップ304:一方、STB100では、Kw暗号化手段107が、現在使用中のコントロールキーKc[3]を用いて、ワークキーKwを暗号化したKc[3](Kw)を記録装置400に転送する。このKc[3](Kw)は、VTR装置200に転送したものと同じである。

【0090】ステップ305:記録装置400での、Kc[3](Kw)の解読動作は、ステップ108の内容と同じである。

ステップ306:暗号化されたAVデータの転送動作は、ステップ109の内容と同じである。

【0091】ステップ307:記録装置400での、AVデータの解読動作は、ステップ110の内容と同じである。

【0092】次に、コントロールキーKc[3]が更新される場合の動作は、上記ステップ201~208での説明において、Kc[0]をKc[2]と読み替え、Kc[1]をKc[3]と読み替え、かつ、乱数Kc'[1]を乱数Kc'[3]と読み替えたものと同じである。

【0093】ここで生成されるコントロールキーKc[4]は、数2のnに3を代入することにより次のように表せる。図2では、乱数Kc'[3]の転送に符号605を付した。

【0094】

【数4】

$Kc[4] = f_i(Kc'[3], Kc[2], Kc[3])$

この様に、途中からAVデータの転送を受ける端末装置が現れて、受信端末が増加しても、STB100が使用するコントロールキーは、受信端末装置の数に関係なく共通したものとなる。

【0095】これにより、不正者が、たまたま、これまで使用されてきたコントロールキーの内、いずれか一つを、例えば、総当たり計算等により解いたとしても、それまでのコントロールキーの履歴と、それとは別の乱数との組み合わせにより、コントロールキーが生成されるため、不正解読されたコントロールキー以降に生成されたコントロールキーが連鎖的に解かれてしまうことを防止出来る。

【0096】又、コントロールキーの更新に使用する乱

数Kc'が、不正者により傍受されたとしても、それ以前のコントロールキーの履歴が分からなければ、コントロールキーの解読は不可能である。

【0097】尚、上記実施の形態では、先に発生させた乱数と、過去のコントロールキーKcとを利用して、関数fi(第1の関数)により新たなコントロールキーKcを生成する場合について述べたが、これに限らず例えば、次の様な構成のデータ送信装置としても良い。即ち、具体的には、図3に示す様に、上記Kc生成手段106に代えて、(1)新たなコントロールキーKcを生成するコントロールキー生成手段1106と、上記乱数発生手段104に代えて、(2)過去に生成されたコントロールキーKcの全部又は一部と前記新たに生成されたコントロールキーKcと、それらを変数とする第2の関数Fiとを利用して、秘密要素Kc'を生成する秘密要素生成手段1104とを備え、前記コントロールキーKcが新たに更新される場合、前記秘密要素Kc'を、前記第2の関数の逆関数F⁻¹iを有するデータ受信装置1200に転送する構成のデータ送信装置1100であっても良い。一方、データ受信装置1200には、図3に示すように、第2関数選択手段1103が有する複数個の第2関数に対応する逆関数を備えた逆関数選択手段1204が設けられている。この逆関数選択手段1204は、受信側認証手段202からの関数識別子iを得て、それに対応する逆関数F⁻¹iを選択し、Kc生成手段205へ送る。Kc生成手段205は、送られてきた逆関数F⁻¹iを用いて、受信側認証手段202からの秘密要素Kc'と過去のコントロールキーKcを変数として、上記と同様に新たなコントロールキーKcを生成する。

【0098】又、上記実施の形態では、認証が成立した場合、初回の転送601(図2参照)で、ワークキーKwの暗号化に最初に使用するコントロールキーKc[1]と、そのコントロールキーの更新に利用するキーKc[0]とを暗号化して転送する場合について述べたが、これに限らず例えば、データ受信装置が有する第1の関数(例えば、関数fi)または上記逆関数F⁻¹iの変数がコントロールキーKcを生成するのに不足している時期においては、前記コントロールキーKcを含む暗号情報を初期情報として、前記データ受信装置に転送する構成のデータ送信装置であっても良い。即ち、具体的には、例えば、図4に示すように、STB2100は、転送1602において、Ksa(Kc[1]、Kc[2])を転送する。転送1602では、すでに行った認証・鍵交換により生成されたサブキーKsaをそのまま使用するの、新たなサブキーの生成作業は不要である。データ受信装置としてのVTR装置2200は、転送されてきたKsa(Kc[1]、Kc[2])を解読し、Kc[2]を抽出する。

【0099】又、これとは別の例として、データ受信装

置が有する第1の関数 f_i 又は上記逆関数 F^{-1}_i の変数が、コントロールキー K_c を生成するのに不足している時期においては、秘密要素（例えば、乱数 K_c' ）を含む前記不足している変数を初期情報として前記データ受信装置に転送する構成のデータ送信装置であってもよい。即ち、具体的には、図5に示すように、例えば、上記実施の形態の（数2）を利用した場合について述べると、次の式（数5）により表せるコントロールキー K_c が、双方の装置において、関数 f_i を利用して生成されるものである。

【0100】

【数5】

$K_c[1] = f_i(K_c'[0], K_c[-1], K_c[0])$
 ここで、 $K_c'[0]$ は、データ送信装置で発生された乱数等の秘密要素であり、 $K_c[-1]$ 、 $K_c[0]$ は、それまでに未使用のコントロールキーである。これら未使用のコントロールキーは、乱数として発生させても良いし、予め、内蔵されている複数個の中から抽出しても良い。この場合、図5に示す転送2601において、データ送信装置としてのSTB3100からデータ受信装置としてのVTR装置3200に対して、コントロールキー $K_c[1]$ の生成に必要な変数として、 $K_c'[0]$ と $K_c[-1]$ と $K_c[0]$ とをサブキーにより暗号化して転送する必要がある。

【0101】又、これとは別の例として、データ受信装置が有する第1の関数又は上記逆関数の変数が、コントロールキー K_c を生成するのに不足している時期の内、

(1) 前半においては、前記コントロールキー K_c を含む暗号情報を初期前半情報として、又、(2) 後半においては、前記秘密要素を含む前記不足している変数を初期後半情報として前記データ受信装置に転送する構成のデータ送信装置であってもよい。即ち、具体的には、図2の転送601に代えて、 $K_{sa}(K_c[1])$ を転送し、同図の転送602に代えて、秘密要素としての $K_c'[1]$ と、上記不足している変数としての $K_c[0]$ とを転送するものである。これにより、転送601の結果、データ受信装置において $K_c[1]$ が抽出され、最初のコントロールキーとして使用される。又、データ受信装置では、この様にして抽出されたコントロールキー $K_c[1]$ と、転送602により入手した $K_c'[1]$ 及び $K_c[0]$ とを変数として、関数 f_i により次のコントロールキー $K_c[2]$ を生成する。

【0102】又、上記実施の形態では、 K_c 生成関数を予め複数個有しており、その中から一つを選択して使用する場合について述べたが、これに限らず例えば、認証動作の際に、使用する関数そのものを転送する構成でも良いし、あるいは、関数は、はじめから固定されていても良い。

【0103】又、上記実施の形態では、先に発生させた乱数と、過去のコントロールキー K_c とを利用して、関

数 f_i （第1の関数）により新たなコントロールキー K_c を生成する場合について述べたが、これに限らず例えば、新たなコントロールキー K_c を生成するコントロールキー生成手段と、過去に生成されたコントロールキー K_c の全部又は一部と前記新たに生成されたコントロールキー K_c と、それらを変数とする第2の関数とを利用して、秘密要素を生成する秘密要素生成手段とを備え、前記コントロールキー K_c が新たに更新される場合、前記秘密要素を、前記第2の関数の逆関数を有するデータ受信装置に転送する構成のデータ送信装置であっても良い。

【0104】又、上記実施の形態では、新たなコントロールキー K_c を生成する際、コントロールキー K_c の履歴として、1つ前と2つ前のものを変数として用いる場合について述べたが、これに限らず例えば、過去に使用したコントロールキーであれば、2つ前と3つ前、若しくは、1つ前と3つ前等どれでも良い。又、過去のコントロールキー K_c であれば、その個数は、2個に限らず、例えば、1個以上であれば、幾つでも良く、記憶容量が確保出来るならば、過去に使用した全てのコントロールキーを用いてもかまわない。

【0105】又、以上述べた実施の形態の何れか一つに記載の各手段またはステップの全部又は一部の手段またはステップをコンピュータに実行させるためのプログラムを記録した磁気記録媒体や光記録媒体などを作成し、これを利用して上記と同様の動作を実行させることも出来る。この場合も上記と同様の効果を発揮する。

【0106】又、上記実施の形態の各手段又はステップの処理動作は、コンピュータを用いてプログラムの働きにより、ソフトウェア的に実現してもよいし、あるいは、上記処理動作をコンピュータを使用せずに特有の回路構成により、ハード的に実現してもよい。

【0107】

【発明の効果】以上述べたところから明らかなように本発明は、従来に比べて実質上の負担を増やすことなくコントロールキーの秘密保持についての信頼性を従来に比べてより一層向上させることが出来るという長所を有する。

【図面の簡単な説明】

【図1】本発明の一実施の形態におけるデータ送信装置及びデータ受信装置の構成を示す構成図

【図2】同実施の形態において、コントロールキーの更新に伴い行われる、STBから受信端末装置への転送の状況を中心に示した模式図

【図3】本発明の他の実施の形態におけるデータ送信装置及びデータ受信装置の構成を示す構成図

【図4】本発明の別の実施の形態において、コントロールキーの更新に伴い行われる、STBから受信端末装置への転送の状況を中心に示した模式図

【図5】本発明のさらに別の実施の形態において、コン

トロールキーの更新に伴い行われる、STBから受信端末装置への転送の状況を中心にした模式図

【図6】従来のデータ送信装置及びデータ受信装置の構成を示す構成図

【符号の説明】

100 STB

101 暗号化手段

102 送信側認証手段

103 Kc生成関数選択手段

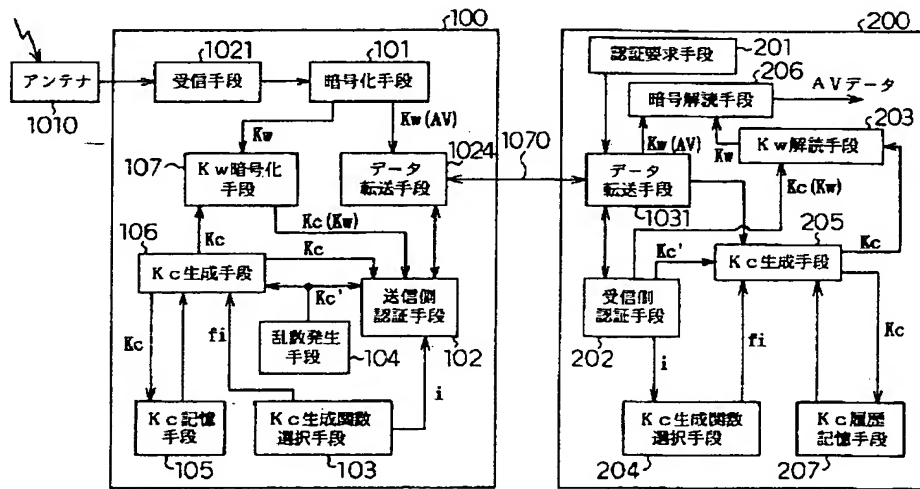
104 乱数発生手段

105 Kc記憶手段

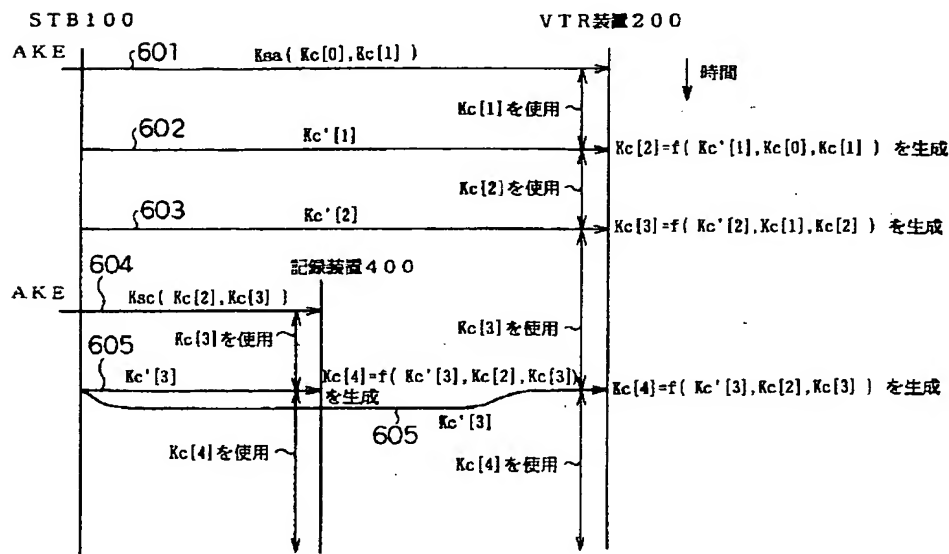
106 Kc生成手段

107 Kw暗号化手段

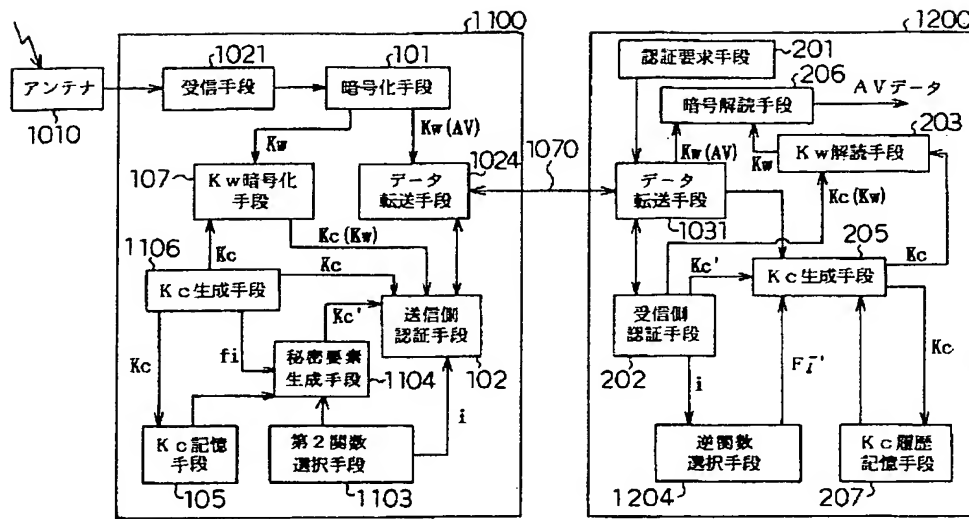
【図1】



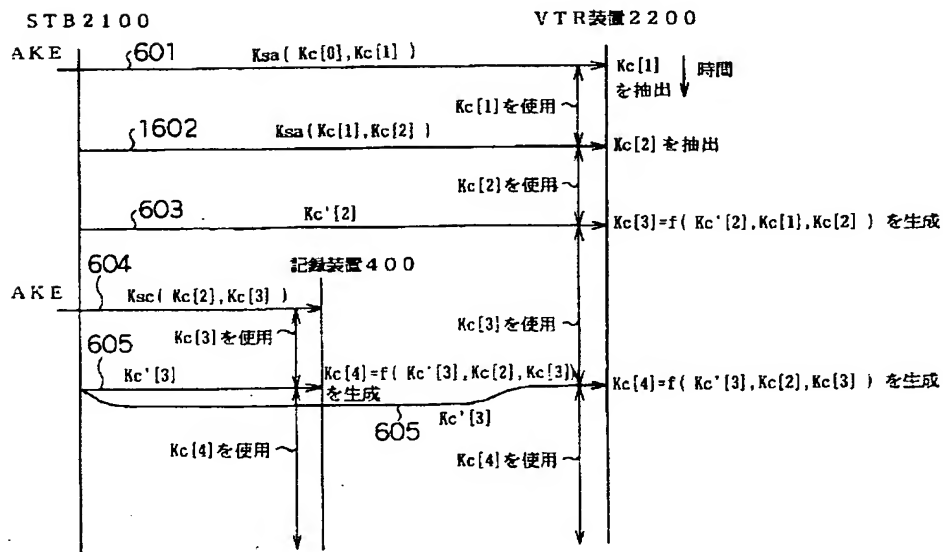
【図2】



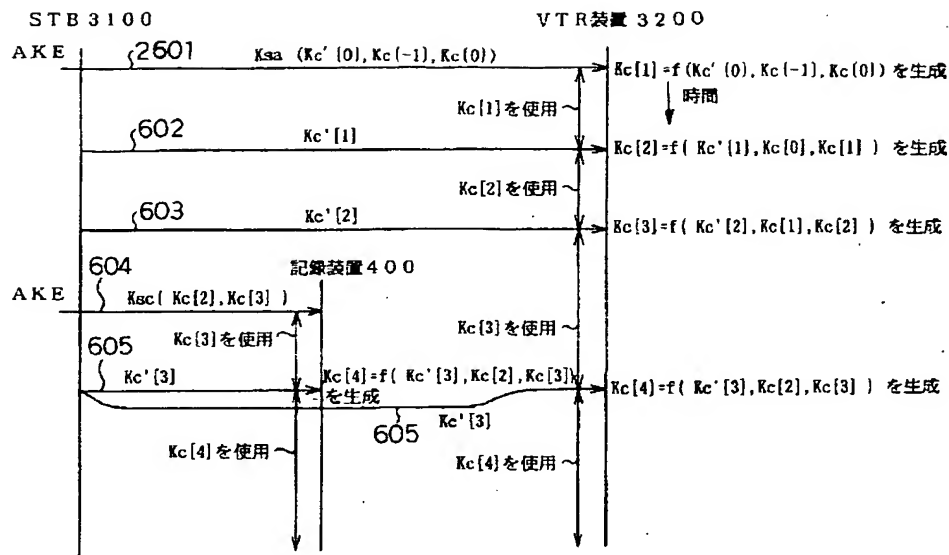
【図3】



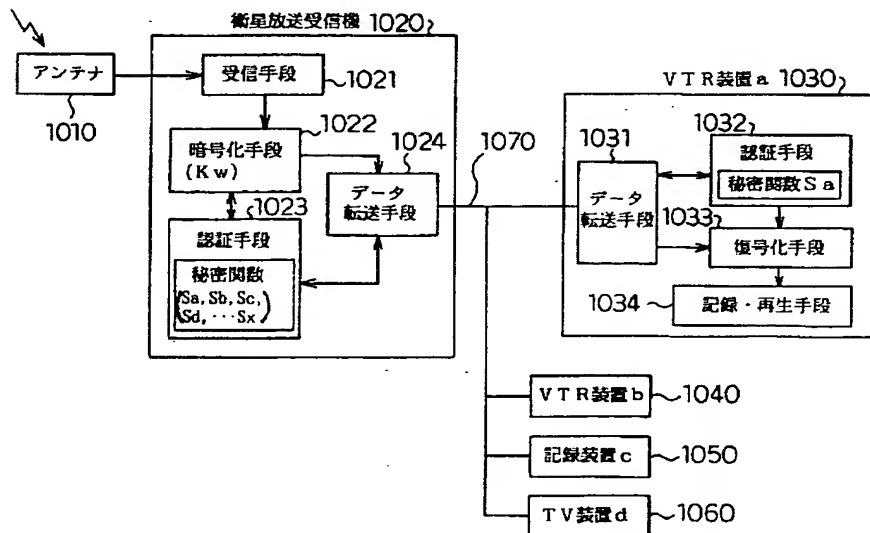
【図4】



【図5】



【図6】



フロントページの続き

(72)発明者 後藤 昌一
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 武知 秀明
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.